PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-315036
(43)Date of publication of application : 08.11.1994

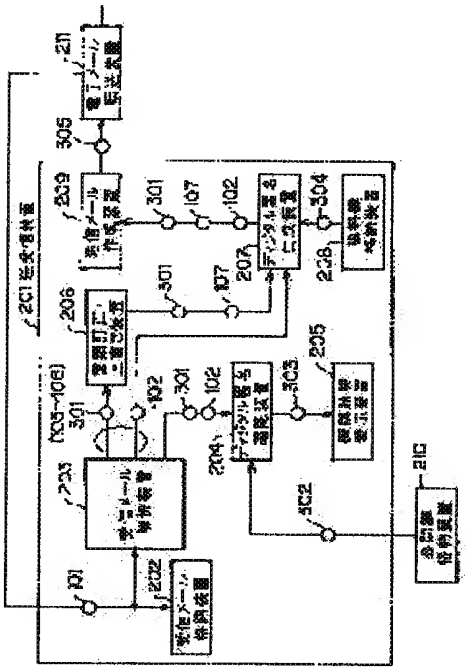
(51)Int.Cl. H04L 12/54
H04L 12/58
G06F 13/00
G06F 15/21
H04L 9/32

(21)Application number : 05-102676
(22)Date of filing : 28.04.1993

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MOTOIKE SACHIKO

(54) ELECTRONIC MAIL SYSTEM WITH DIGITAL SIGNATURE

(57)Abstract:
PURPOSE: To receive a document described and signed by plural persons as electronic mail with digital signature, to confirm the priority and further to transmit it as the electronic mail with digital signature after being additionally signed.
CONSTITUTION: A signature information file 102 and plural entity files 103-106 are made into one piece of document data and defined as the target of transmission/reception, after the reception, the document is analyzed by a received mail analyzer 203, and the digital signature applied to the entity files is confirmed by a digital signature confirming device 204 by using a public key 302 of a signing persons. Further, a new entity file 107 is generated by copying the latest entity file, thereby the entity file is additionally described by a document correcting/overwriting device 206, and the digital signature is generated by a digital signature generator 207 by using a public key 304 of an additional describing person to all the entity files.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－315036

(43)公開日　平成６年(1994)11月８日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/54					
	12/58					
Ｇ０６Ｆ	13/00	３５１	Ｇ　7368－5B			
			8732－5K	Ｈ０４Ｌ　11/20	１０１　Ｂ	
			8949－5K	9/00	Ａ	

審査請求　未請求　請求項の数３　ＯＬ　（全　８　頁）　最終頁に続く

(21)出願番号　特願平5－102676

(22)出願日　平成５年(1993)４月28日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　本　池　祥　子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

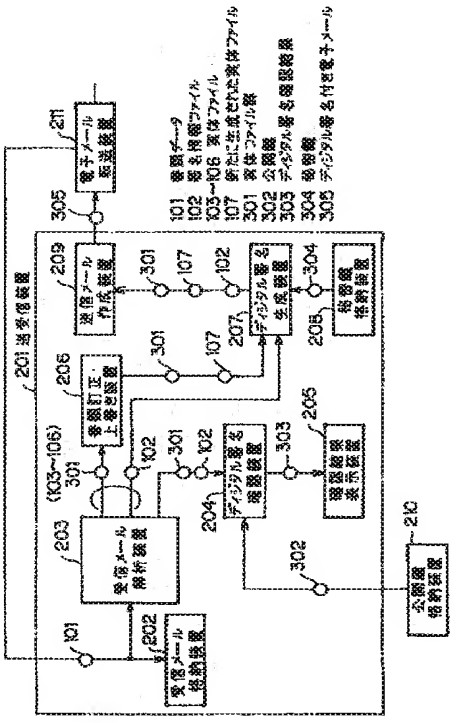
(74)代理人　弁理士　蔵合　正博

(54)【発明の名称】　ディジタル署名付き電子メールシステム

(57)【要約】

【目的】　複数人によって記入され、署名された書類をディジタル署名付き電子メールとして受信し、その正当性を確認し、さらに追記して署名を施した上、ディジタル署名付き電子メールとして送信できるようにする。

【構成】　署名情報ファイル１０２と複数の実体ファイル１０３～１０６を一つの書類データ１０１として送受信の対象とし、受信後に書類を受信メール解析装置２０３で解析して実体ファイルに施されたディジタル署名を署名者の公開鍵３０２を用いてディジタル署名確認装置２０４により確認する。さらに最新の実体ファイルをコピーして新たな実体ファイル１０７を生成し、追加記入はこの実体ファイルに対して書類訂正・上書き装置２０６で行ない、ディジタル署名はすべての実体ファイルに対して追加記入者の秘密鍵３０４を用いてディジタル署名生成装置２０７により生成する。



1

【特許請求の範囲】

【請求項１】　複数ファイルをまとめて一つの電子メールとして取り扱うことが可能な電子メールシステムにおいて、電子メールを構成する複数ファイルのうちの一つを署名情報ファイルとし、残りを実体ファイルとし、署名情報ファイルには実体ファイル間に定義される論理的な依存関係とその依存関係に応じてそれぞれの実体ファイルに対して施されたディジタル署名の値とを記録して伝送する送受信装置を備えたディジタル署名付き電子メールシステム。

【請求項２】　送受信装置が、受信メールから署名情報ファイルと実体ファイルとを分離する受信メール解析手段と、前記受信メール解析手段から得られた実体ファイルと署名情報ファイルと署名者の公開鍵を用いて実体ファイルに施された複数人のディジタル署名の正当性を確認するディジタル署名確認手段とを備えた請求項１記載のディジタル署名付き電子メールシステム。

【請求項３】　送受信装置が、複数人のディジタル署名の施された受信メールに受信者が追加記入を行なって新たな実体ファイルを作成する訂正・上書き手段と、追加記入の加えられた受信メールと受信者の秘密鍵を用いて受信者のディジタル署名を生成するとともに、署名情報ファイルに実体ファイル間の論理構造とディジタル署名の値を記入するディジタル署名作成手段と、署名情報ファイルと実体ファイルとをまとめて送信メールを作成する送信メール作成手段とを備えた請求項２記載のディジタル署名付き電子メールシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、複数の利用者の間でディジタル署名を施した電子メールの送受信を行うディジタル署名付き電子メールシステムに関するものである。

【０００２】

【従来の技術】従来、電子メールシステムでは、公開鍵暗号方式によるディジタル署名を施した電子メールが用いられている。以下、従来のこの種の電子メールシステムについて、図面を参照しながら説明する。

【０００３】図５は従来のディジタル署名付き電子メールシステムの構成を示すものである。図５において、１はディジタル署名付き電子メールシステムのうち、送信用の電子メールにディジタル署名を施して送信する送信側装置であり、２は送信者の秘密鍵格納装置、３は送信メール作成装置、４はディジタル署名生成装置である。５はディジタル署名付き電子メールを転送する電子メール転送装置である。６は従来例におけるディジタル署名付き電子メールシステムのうち、電子メールを受信してディジタル署名の確認を行なう受信側装置であり、７は受信メール格納装置、８はディジタル署名確認装置、９はディジタル署名確認装置８の結果を受けてディジタル署名が正しいかどうかを表示する確認結果表示装置である。１０はディジタル署名を確認するのに必要な送信者の公開鍵を格納しておく、公開鍵格納装置である。

2

【０００４】以上のように構成されたディジタル署名付き電子メールシステムにおいて、送信者Ａが受信者Ｂに対してディジタル署名付きの電子メールを送付し、受信者Ｂが受け取った電子メールのディジタル署名を確認する場合の動作について説明する。

【０００５】送信者Ａが送信メール作成装置３を用いて受信者Ｂ宛の電子メール１１を作成後、ディジタル署名を付加して送信することを指示すると、電子メール１１はディジタル署名生成装置４に送られる。ディジタル署名生成装置４は、送信者Ａの秘密鍵１２を秘密鍵格納装置２から得て、電子メール１１の内容からディジタル署名の値を計算し、それを電子メール１１に付加したディジタル署名付き電子メール１３を電子メール転送装置５に送る。これにより、送信者Ａはディジタル署名付き電子メールを受信者Ｂ宛に送信することができる。

【０００６】受信者Ｂ宛のディジタル署名付き電子メール１３は、受信者Ｂの受信メール格納装置７に格納される。受信者Ｂがディジタル署名付き電子メール１３の正当性の確認を指示すると、ディジタル署名付き電子メール１３は、ディジタル署名確認装置８に送られる。ディジタル署名確認装置８は、送信者Ａの公開鍵１４を公開鍵格納装置１０から得て、ディジタル署名付き電子メール１３のディジタル署名の正当性を計算し、その結果を示すデータ１５を確認結果表示装置９に送る。確認結果表示装置９は、データ１５をもとに、正当性が確認されたか否かを受信者Ｂに表示する。

【０００７】以上が、従来のディジタル署名付き電子メールシステムにおける送信者Ａが受信者Ｂに対してディジタル署名付きの電子メールを送付し、受信者Ｂが受け取った電子メールのディジタル署名を確認する場合の動作である。

【０００８】この方式は、送信者が複数の相手に対して同時にディジタル署名を施したメールを送信することを可能とし、さらにまた、署名付き電子メールをそのまま他の利用者に転送することで、元のメールの内容が正しく伝えられることを保証するものである。

【０００９】

【発明が解決しようとする課題】しかしながら、上記従来の構成においては、決裁願や稟議書のように複数人が書き込みを行ないながら転送していく書類に対して、個々人が転送途中の同一書類への追加記入とディジタル署名を施しながら書類を送信することは、書類への追加記入そのものが、それまでの署名者のディジタル署名の正当性の確認を不可能とすることと等しい行為であることから、結果として電子メールにおけるディジタル署名の有効性を保持できないという問題点を有していた。

【００１０】本発明は、上記従来の問題点を解決するもので、決裁願や稟議書のように複数人が書き込みを行な

い、かつ署名を施す書類であっても、ディジタル署名の有効性を保持しながら電子メールによって転送することのできるディジタル署名付き電子メールシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために、本発明のディジタル署名付き電子メールシステムは、第一に、複数ファイルをまとめて一つの電子メールとして取り扱うことが可能な電子メールシステムにおいて、電子メールを構成する複数ファイルのうちの一つを署名情報ファイルとし、残りを実体ファイルとし、署名情報ファイルには、実体ファイル間に定義される論理的な依存関係とその依存関係に応じてそれぞれの実体ファイルに対して施されたディジタル署名の値とを記録して伝送する送受信装置を備えたものである。

【００１２】また第二に、上記構成において、受信メールから署名情報ファイルと実体ファイルとを分離する受信メール解析手段と、受信メールを解析して得られた実体ファイルと署名情報ファイルと署名者の公開鍵を用いて実体ファイルに施された複数人のディジタル署名の正当性を確認するディジタル署名確認手段とを備えたものである。

【００１３】また第三に、上記構成において、複数人のディジタル署名の施された受信メールに受信者が追加記入を行なって新たな実体ファイルを作成する訂正・上書き手段と、追加記入の加えられた受信メールと受信者の秘密鍵を用いて受信者のディジタル署名を生成するとともに、署名情報ファイルに実体ファイル間の論理構造とディジタル署名の値を記入するディジタル署名生成手段と、署名情報ファイルと実体ファイルとをまとめて送信メールを作成する送信メール作成手段とを備えたものである。

【００１４】

【作用】本発明は、上記構成によって、複数ファイルを論理的に一つの書類と見なし、書類を構成する実体ファイルと、その実体ファイルが論理的に依存している他の実体ファイルに対してそれぞれの記入者のディジタル署名を施すことにより、決裁願や稟議書のように、複数人がそれぞれの場所を記入した上で捺印し、次の担当者に書類を回すような処理と同等の処理を、ディジタル署名を用いて電子メールシステム上にて行なうことができる。

【００１５】

【実施例】以下、本発明の一実施例について、図面を参照しながら説明する。図１は本発明の一実施例におけるディジタル署名付き電子メールシステムにおいて、送受信の対象とする書類のデータ構成を示す図である。図１において、１０１は書類データ全体を示し、１０２から１０６は書類データ１０１を構成する複数のファイルである。１０２は書類データ１０１の論理構造と、１０３から１０６のそれぞれの実体ファイルに対して施されたディジタル署名の値を記録する署名情報ファイル、１０３から１０６は書類データ１０１の実体に相当する実体ファイルである。本図は実体ファイルが４つの場合を示しているが、その個数は一つ以上であればいくつでも良い。

【００１６】図２は本発明の一実施例におけるディジタル署名付き電子メールシステムの装置構成を示す図である。図２において、２０１は本実施例のディジタル署名付き電子メールシステムのうち、特定の利用者ごとに必要となる送受信装置を示している。２０２は受信メール格納装置、２０３は受信メール解析装置、２０４はディジタル署名確認装置、２０５は確認結果表示装置、２０６は書類訂正・上書き装置、２０７はディジタル署名生成装置、２０８は秘密鍵格納装置、２０９は送信メール作成装置である。２１０は公開鍵格納装置、２１１は電子メール転送装置であり、これらはすべての利用者に共通の装置である。また、１０１、１０２はそれぞれ図１で示した書類データ、署名情報ファイルを示している。３０１は書類データ１０１を構成する実体ファイル群、１０７は追加記入により発生した新しい実体ファイル、３０２は署名情報ファイル１０２に記述されている署名の作成者の公開鍵、３０３はディジタル署名の確認結果を示すデータ、３０４は利用者の秘密鍵、３０５はディジタル署名付き電子メールである。

【００１７】次に、上記装置における動作について説明するが、その前にまず、本実施例において送受信の対象となる書類の構成について、図１を用いて説明する。図１において、書類データ１０１は、複数のファイル１０２～１０６が論理的に一つの書類を構成しているファイル１０３から１０６までは、それぞれ利用者Ａ、Ｂ、Ｃ、Ｄの作成した実体ファイルであり、それぞれの利用者の署名の値が、署名情報ファイル１０２に格納されている。ＣＣＩＴＴのＸ．４００に準拠したメールシステムにおいては、複数ファイルをまとめて送信するプロトコルが提供されているため、送信側・受信側でともに複数ファイルを論理的にまとめて一つとして扱うことができる。

【００１８】実体ファイル１０３から実体ファイル１０６と、それぞれの利用者の署名の値との間には以下に示すような参照関係が存在する。

【００１９】実体ファイル１０３は、利用者Ａが作成したファイルであり、Ａの署名は実体ファイル１０３のみに施されたもの、即ち実体ファイル１０３のみを用いてＡの秘密鍵によって計算されたディジタル署名である。

【００２０】これに対し、実体ファイル１０４は、実体ファイル１０３をコピーしたファイルに、利用者Ｂが追加記入や訂正を行なって作成したファイルであり、Ｂの署名は、これら二つの実体ファイル１０３と実体ファイル１０４とに施されたもの、即ち実体ファイル１０３と

5

実体ファイル１０４とを用いてＢの秘密鍵によって計算されたディジタル署名である。

【００２１】以下同様に、実体ファイル１０５は、実体ファイル１０４をコピーしたファイルに利用者Ｃが追加記入や訂正を行なったもの、実体ファイル１０６は、実体ファイル１０５をコピーしたファイルに利用者Ｄが追加記入や訂正を行なったものであり、また、Ｃの署名は、実体ファイル１０３から実体ファイル１０５までの三つのファイルに施されたもの、Ｄの署名は、実体ファイル１０３から実体ファイル１０６までの四つのファイルに施されたものである。

【００２２】本実施例では、送受信の対象として、このような論理構造を持ったファイルの集まりを書類として利用する。

【００２３】次に、図２を用いて書類データ１０１を受け取った利用者Ｅが書類の正当性を確認し、追加記入・修正を行ない、さらに次の利用者に書類を転送する方法を説明する。

【００２４】利用者Ｅが電子メール転送装置３１を介して利用者Ｄから受け取ったディジタル署名付き電子メールの書類データ１０１は、一旦受信メール格納装置２０２に格納され、書類データ１０１の正当性の確認を行なうために、受信メール解析装置２０３に送られる。受信メール解析装置２０３では、書類データ１０１を解析し、署名情報ファイル１０２と、四つの実体ファイル１０３、１０４、１０５、１０６からなる実体ファイル群３０１とをディジタル署名確認装置２０４に出力する。署名情報ファイル１０２には、図１を用いて説明したように、利用者Ａから利用者Ｄのそれぞれの署名の値と各実体ファイルの間に存在する論理構造が記述されている。

【００２５】ディジタル署名確認装置２０４は、署名情報ファイル１０２に記述されている実体ファイル間の論理構造に従い、公開鍵格納装置２００から利用者Ａから利用者Ｄのそれぞれの公開鍵３０２を得て、以下のような順序で署名の正当性の確認を行ない、その結果を送受信装置２０１内の図示されないメモリに記憶しておく。

【００２６】まず、実体ファイル１０３の正当性を、署名情報ファイル１０２に記述されているＡの署名の値と公開鍵格納装置２１０からのＡの公開鍵を用いて確認する。これにより、書類データ１０１を構成する実体ファイルのうち、もともと利用者Ａが作成した実体ファイル１０３の正当性を確認することができる。

【００２７】次に、実体ファイル１０４の正当性を、署名情報ファイル１０２に記述されているＢの署名の値と実体ファイル１０３とＢの公開鍵を用いて確認する。Ｂの署名の値は、実体ファイル１０３、１０４の双方を用いて計算されているためである。これにより、書類データ１０１を構成する実体ファイルのうち、利用者Ｂは利用者Ａの作成した実体ファイル１０３を用いて実体ファイル１０４を作成し、署名したことが確認でき、実体ファイル１０４自身の正当性と、実体ファイル１０３と１０４との依存関係についての正当性を確認することができる。

6

【００２８】以下同様に、実体ファイル１０５、１０６それぞれの正当性と、実体ファイル１０３から１０５の依存関係、実体ファイル１０３から１０６の依存関係についての正当性を順次確認することができ、最終的に、全体として書類データ１０１が利用者Ａから利用者Ｄによって順次正当に作成されたものであることを確認することができる。確認結果を示すデータ３０３は確認結果表示装置２５に送られ、利用者Ｅは署名の正当性を確認することができる。

【００２９】さて、利用者Ｅがこのような書類データ１０１に対して、追加記入の開始を指示すると、書類訂正・上書き装置２０６は、実体ファイル群３０１を得て、最新の実体ファイルである１０６をコピーし、利用者Ｅに対して追加記入可能な状態とする。利用者Ｅがこれに対して追加記入を行ない、追加記入の終了を指示すると、利用者Ｅによって新しく作成された実体ファイル１０７と実体ファイル群３０１、署名情報ファイル１０２は、ディジタル署名生成装置２０７に送られる。ディジタル署名生成装置２０７は、実体ファイル群３０１と実体ファイル１０７に対して、秘密鍵格納装置２０８から得た利用者Ｅの秘密鍵３０４を用いて署名の値を計算し、その結果を署名情報ファイル１０２に書き込み、また、実体ファイル１０３から１０７の間に存在する論理構造をも同時に書き込む。

【００３０】最終的に、送信メール作成装置２０９は、署名情報ファイル１０２と、実体ファイル１０３から１０７によって構成される送信メール３０５を形成し、電子メール転送装置２１１に送信メールを渡す。

【００３１】このようにして、利用者Ｅは、書類データ１０１の正当性を確認することができ、また、さらに追加記入の上、利用者Ｅ自身の署名を施し、他の利用者にディジタル署名付き電子メールとして送信することができる。

【００３２】図３および図４は上記実施例の動作より具体的に示したものである。図３において、１００は書類データ１０１を従来形式の書類としてイメージ化したもので、ここでは決裁願を例にしている。いま、起案者Ａ（松下）が、ワークステーション３台の購入を申請するために決裁願を起案したものとする。これを電子メールにより上司の係長に転送する場合、申請内容を表わした実体ファイル１０３と、実体ファイル１０３を基に計算された起案者Ａの印鑑に相当する署名の値および実体ファイル間の論理構造（この場合はファイルがひとつなので、自身のファイル名）が記述された署名情報ファイル１０２とからなる書類データ１０１が作成される。

【００３３】図４において、このような書類データに基

づく電子メールを係長が起案者Ａから受信すると、係長はこれを受信メール解析装置２０３により実体ファイル１０３と署名情報ファイル１０２とに分離して、ディジタル署名確認装置２０４により署名の有効性を確認するとともに、内容を確認して、ワークステーション３台は無理なので、これを書類訂正・上書き装置２０６により２台に訂正して、実体ファイル１０３を基にして新たな実体ファイル１０４を生成するとともに、ディジタル署名生成装置２０７により署名情報ファイル１０２に実体ファイル１０３と１０４を基に計算された係長（木村）の署名の値と実体ファイル間の論理構造（この場合は実体ファイル１０３と１０４との関係）を追加記述して送信メールを作成し、次の課長宛に電子メールで送信する。

【００３４】このようにして受信者が順次実体ファイルを作成し、署名情報ファイルにその署名の値および新たに作成された実体ファイル間の論理構造を追加記述した書類データを作成することにより、最終の決裁者は、起案者以降のすべての実体ファイルの内容および署名を確認することができ、最終判断を的確に行なうための情報を得ることができる。

【００３５】

【発明の効果】以上のように本発明は、実体ファイルと署名情報ファイルから構成される書類データを解析し、署名の正当性を確認するとともに、新たな実体ファイルを追加して、それへの署名を生成して追加記入することにより、複数人によって記入され、また署名された書類をディジタル署名の有効性を保持しながら署名付き電子メールとして送受信することができる。

【図面の簡単な説明】

【図１】本発明の一実施例におけるディジタル署名付き電子メールシステムにおいて送受信の対象とする書類データのデータ構成図

【図２】本発明の一実施例におけるディジタル署名付き電子メールシステムの送受信装置の構成を示すブロック図

【図３】本発明の一実施例におけるディジタル署名付き電子メールシステムの動作を示す模式図

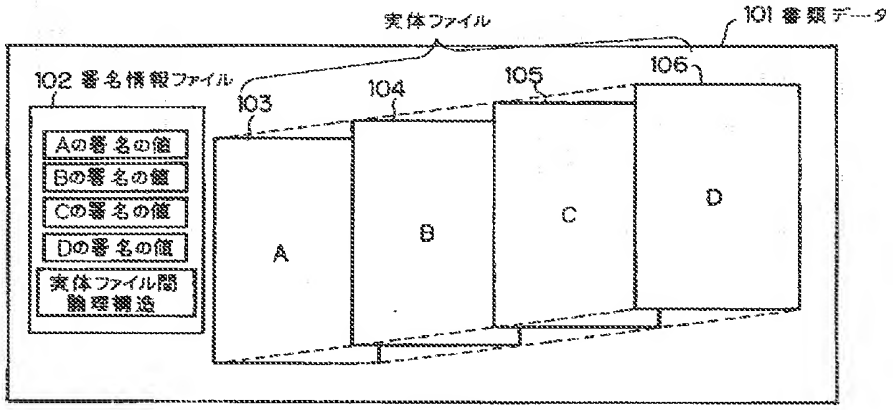
【図４】本発明の一実施例におけるディジタル署名付き電子メールシステムの動作を示す模式図

【図５】従来例におけるディジタル署名付き電子メールシステムのシステム構成図

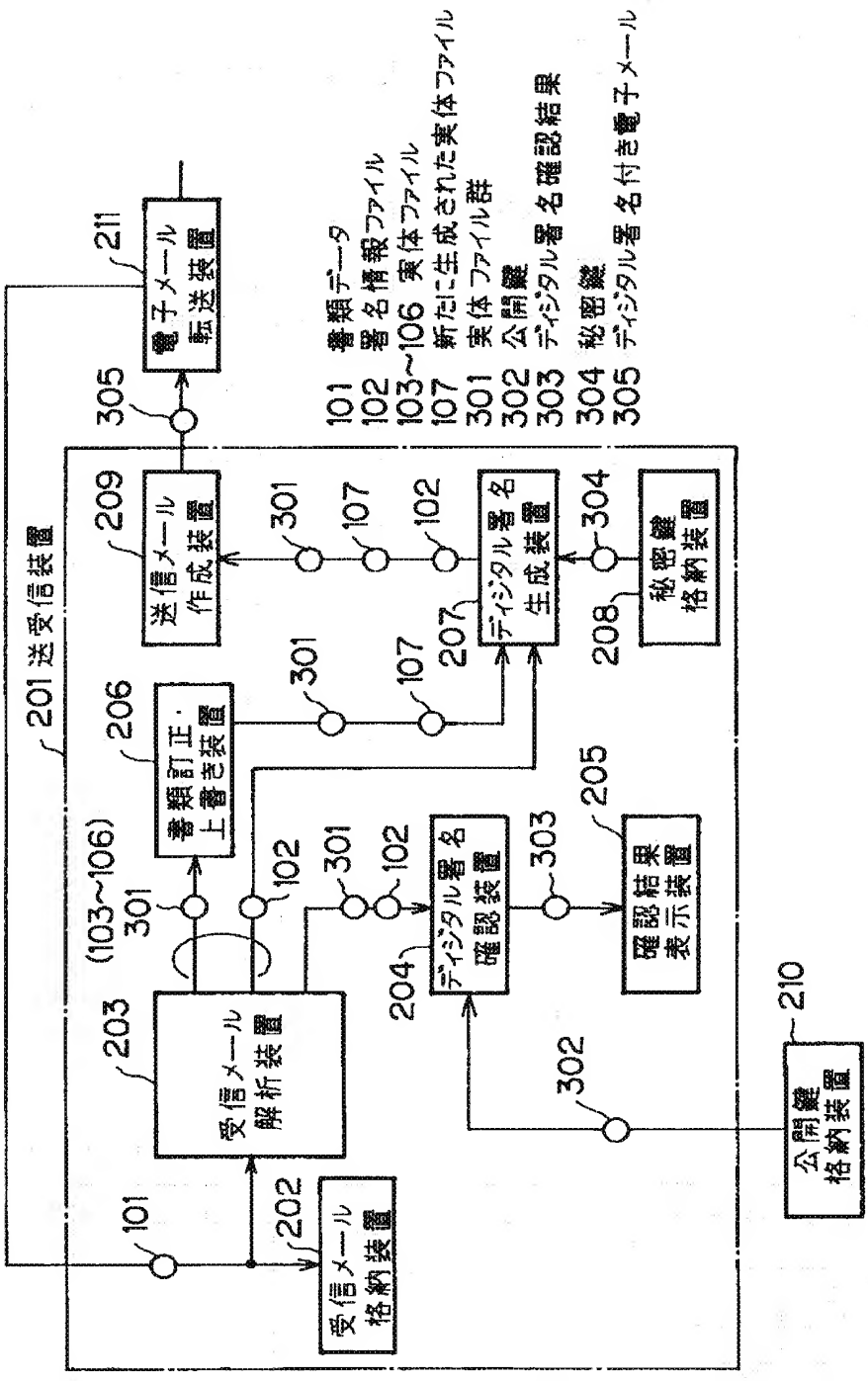
【符号の説明】

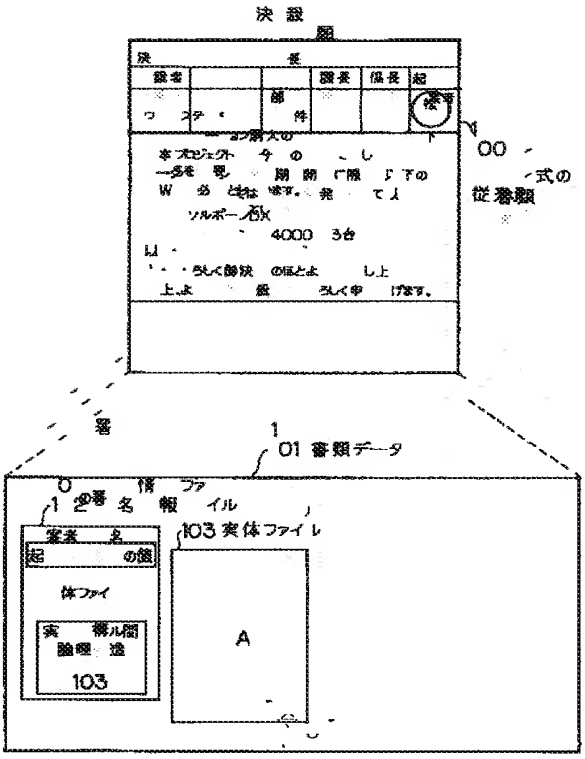
１００　従来形式の書類
１０１　書類
１０２　署名情報ファイル
１０３～１０７　実体ファイル
２０１　送受信装置
２０２　受信メール格納装置
２０３　受信メール解析装置
２０４　ディジタル署名確認装置
２０５　確認結果表示装置
２０６　書類訂正・上書き装置
２０７　ディジタル署名生成装置
２０８　秘密鍵格納装置
２０９　送信メール作成装置
２１０　公開鍵格納装置
２１１　電子メール転送装置
３０１　実体ファイル群
３０２　公開鍵群
３０３　ディジタル署名確認結果
３０４　秘密鍵
３０５　ディジタル署名付き電子メール

【図１】

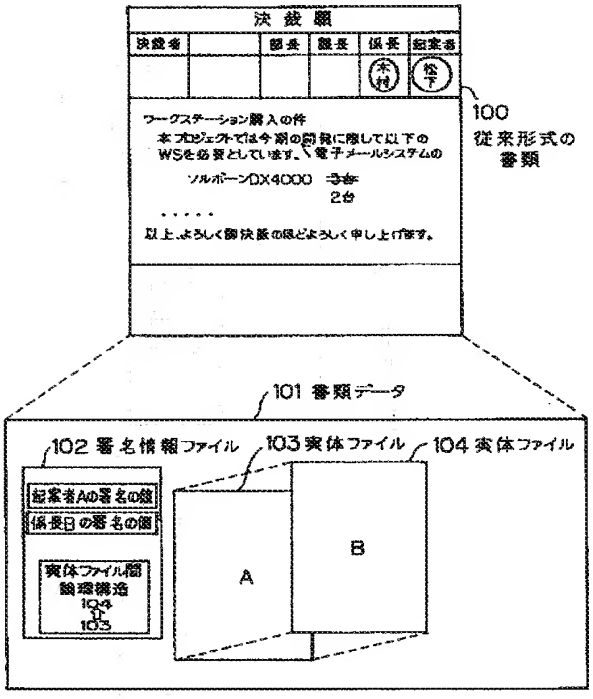


【図2】

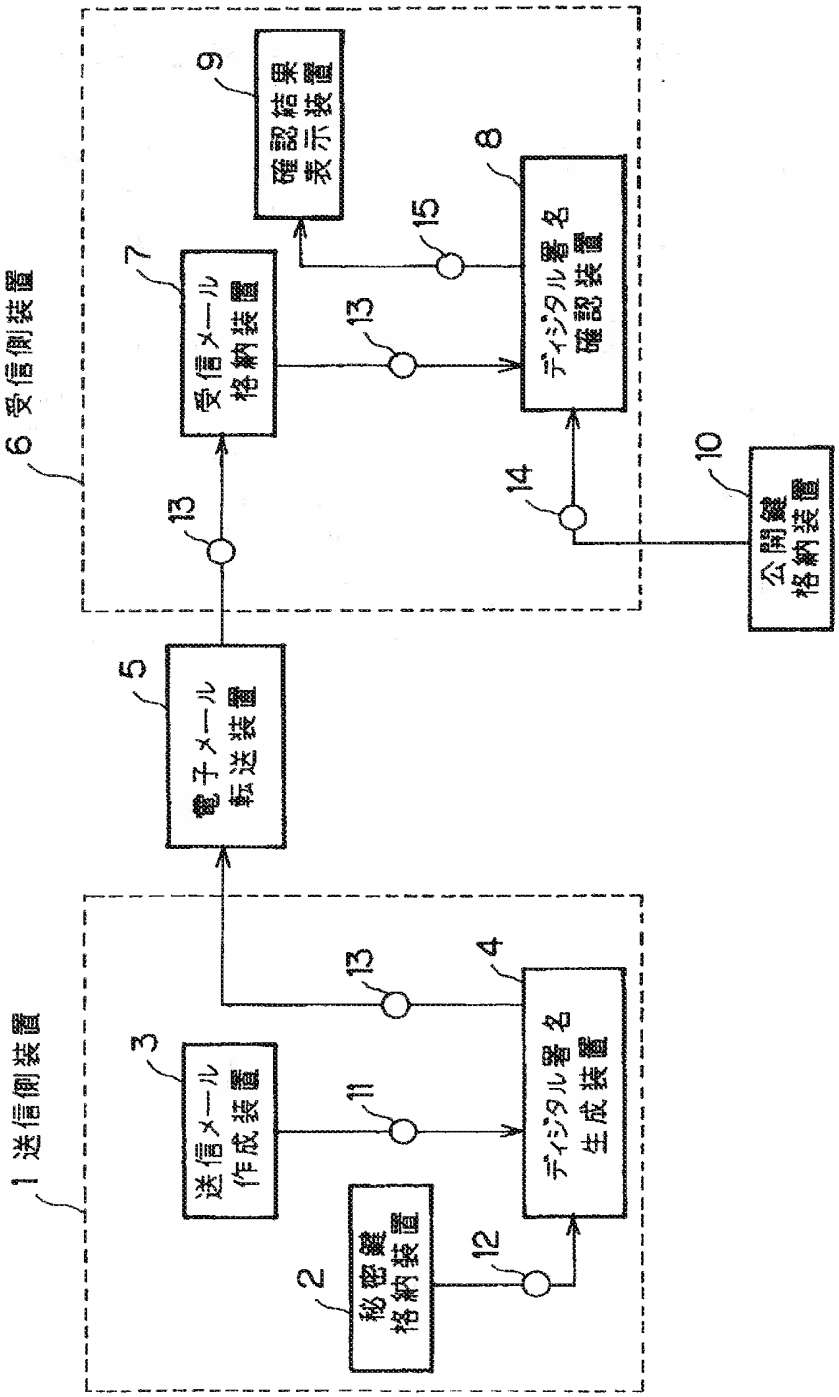

201 送受信装置
101
202
受信メール格納装置
203
受信メール解析装置
(103~106)
301
102
204
ディジタル署名確認装置
303
205
確認結果表示装置
206
書類訂正・上書き装置
207
ディジタル署名生成装置
208
秘密鍵格納装置
209
送信メール作成装置
211
電子メール転送装置
305
210
公開鍵格納装置
302
304
107
101 書類データ
102 署名情報ファイル
103~106 実体ファイル
107 新たに生成された実体ファイル
301 実体ファイル群
302 公開鍵
303 ディジタル署名確認結果
304 秘密鍵
305 ディジタル署名付き電子メール


決 設 願
00
式の
従番類
署
1
01 番類データ
0 情 ァ
1 2 署 名 報 イル
103 実体ファイ ル
A
103

【図４】


決 裁 願
決裁者
部長
課長
係長
起案者
100
従来形式の
番類
101 番類データ
102 署名情報ファイル
103 実体ファイル
104 実体ファイル
起案者Aの署名の領
係長Bの署名の領
実体ファイル間
論理構造
104
103
A
B

【図5】



フロントページの続き

(51) Int. Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
G06F 15/21	340 B	8724－5L		
H04L 9/32				